Department of
INFORMATION
TECHNOLOGY

Maryland Configuration Management Policy

Last Updated: 01/31/2017

Contents

1.0 Introduction

Configuration management is critical to establishing an initial baseline of hardware, software, and firmware components of Enterprise information systems and subsequently controlling and maintaining an accurate inventory of any changes to those systems. The Maryland Department of Information Technology (DoIT) is committed to managing the confidentiality, integrity, and availability of their information technology (IT) networks, systems, and applications (IT Systems) by establishing and enforcing standard baselines within the Enterprise. This allows DoIT to document, authorize, manage, and control system changes and prevent deviation from the established accepted risk.

DoIT will utilize baseline controls standardized by NIST SP 800-53R4 and NIST SP 800-128, and any baseline configuration will consider any available Standard Technical Implementation Guides (STIGs) supplied by Defense Information Systems Agency (DISA) as best practice.

2.0 Document History

This policy supersedes the State of Maryland Information Security Policy (version 3.1, Feb 2013) Section 6.1: Configuration Management and any related policy regarding configuration management declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all information technology assets utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology (DoIT). Information technology assets within the purview of configuration management include any systems and applications with network and enterprise configurations that manage and maintain the reliable operations and security of the device and the information processed on that device.

4.0 Policy

DoIT will designate an **Enterprise Configuration Manager** responsible for coordinating all asset inventory and deployment with the Enterprise Asset Manager and working closely with IT administrators to establish, maintain, manage, and track baseline configurations of IT assets. This role will assist in performing auditing and compliance reviews of IT assets and confidential information. Additionally, the Enterprise Configuration Manager will be responsible for coordinating the **Change Control Board (CCB)** and will track proposed and approved changes to software and hardware configurations.

DoIT will designate an **Enterprise Requirements Manager** who serves as the lead of the Change Control Board (see section 4.1 (A)) and will review the feedback from all stakeholders to decide the course of action given the associated risks and business impact. This role is considered the chief IT and business strategist who coordinates with internal and agency stakeholders regarding proposed changes.

4.1 Establish Change Control Board

DoIT will establish a Change Control Board that will have the collective responsibility and authority to review and approve changes to an information system as outlined within the remainder of this policy. Any agency under the policy authority, but not under direct management, of DoIT will be required to create its own internal Change Control Board and independently comply with the requirements of this policy.

#	Name	Requirement
A	Change Control Board (CCB)	Consists of at least the following five members (B through F below) representing multiple sectors of IT and Cybersecurity relevant to the requested change.
B	Requirements Manager	Designated CCB lead who manages stakeholder requirements: analyzes, traces, and prioritizes proposed changes; and serves as final authority on change requests.
C	Configuration Manager	CCB Coordinator, documents all change requests and approvals (or disapprovals) and ensures all stakeholders are involved in examining the risk and the requirements of proposed changes.
D	Asset Manager	Intermediary between logistics and procurement functions and IT services.
E	Information Assurance Manager or Information System Security Manager (IAM/ISSM)	Information security official who conducts the technical security review to identify potential consequences and risks of proposed changes.
F	Technical Lead	Division lead administrator or engineer who proposes or implements the change. ▪ May be the Networking Lead, System Engineering Lead, Application Administrator Lead, Customer Support Lead, etc. depending on change or configuration requested.

4.2 Establish Baseline Configurations

Agencies must develop, document, and maintain a **baseline configuration** of their information systems according to the requirements listed in the table below.

#	Name	Requirement
A	Establish Baseline Configuration	Develop, document, and maintain a current baseline configuration for information systems.
B	Identify Operating System	Establish standard operating systems and versions within the Enterprise; consolidate to standardized software where applicable to avoid loss of time and effort configuring a large variety of operating systems.
C	Standard Software Loads	Determine the standard loadout of applications and software for device categories.

#	Name	Requirement
		▪ As an example, Microsoft servers may require specific software to always be installed like antivirus, asset management agents, or system management tools; workstations may always require Microsoft Office, Adobe Reader, antivirus, remote access or management tools, etc.
D	Approved Hardware and Software	▪ Maintain list of hardware assets approved for operation on the network based on technical security reviews and standard configurations, e.g., specific printer models or workstations. ▪ Maintain list of approved software, including quantities and total number of licenses based on technical security reviews and mission and business requirements. (See *Asset Management Policy* for license management).
E	Timely Patches and Updates	Update the baseline image and configuration to reflect periodic patching or software updates (See *Patch Management Policy*).
F	Network Topology	Update all physical and logical network topology maps and diagrams to reflect changes in asset allocation and naming.
G	Specific Configuration Settings	▪ Maintain an itemized list or snapshot of specific rules, such as switch configurations, enforced firewall rules, whitelists/blacklists, group policy objects, etc. ▪ Maintain tracking, isolation, and access controls to confidential information to ensure critical data loss is minimized.
H	Monitoring	Implement continuous compliance monitoring using a combination of tools and physical review.
I	Auditing and Compliance	Conduct routine audits on all assets to ensure policies and practices are followed.

4.3 Establish a Configuration Management Process

All agencies under the policy authority of DoIT must establish and implement a Change Control Process, including the identification and implementation of a Change Control Board (described in section 4.1 above). DoIT will establish change control functions for onboarded agencies. The table below lists the basic change control functions that must be implemented.

#	Name	Requirement
A	Change Control Process	Establish a formal, written, process used to request, review, and manage all proposed changes to the IT architecture or to asset configuration.
B	Standardized Change Requests	Create a standardized Change Request Form and database with trackable fields automated for ease of submission, querying, and auditing.
C	Business or Mission Requirement	Identify the driver or requirement for the requested change, such as a requirement for new software or a software upgrade.
D	Point of Contact Approval	Require approval of change requests from the Division manager of the requestor (who will serve as a designated Point of Contact).
E	Risk Categorization	Determine the risk level and impact of the proposed change by identifying the security categorization and integrating the corresponding security controls or mitigations.
F	Testing	Isolate or control testing of changes to ensure no adverse or unidentified consequences result from change.

#	Name	Requirement
G	Rollback	Identify method or procedure for returning system to previous state in the event of failure or unintended consequences of change.
H	Maintenance of Requests	Configuration requests will be maintained for a period of three (3) years and will be used to perform audit and compliance queries.
I	Cadence of Review Board	Establish a cadence for how often the Change Control Board will meet and identify the process to call an emergency meeting, when needed.
J	System Development Lifecycle	Define the configuration items for the information technology assets and identify when in the system development life cycle the configuration items are placed under configuration management (see Section 4.9 below for more information).

Standard versus Non-Standard Changes

Configuration Changes will be identified as one of two types: Standard and Non-Standard.

- Standard changes are considered low-risk changes – these include, but are not limited to, routine security patching and updates to firewall or Intrusion Detection System (IDS) rules. A change request must be submitted to the Configuration Manager indicating the intention to perform the low risk change. The request will be documented and reviewed by the Configuration Manager to ensure the request is properly classified and recorded for auditing purposes.
- Non-Standard changes require approval from the Change Control Board. This process ensures that any risk associated with the change is identified and properly prepared for, that any proposed changes do not cause deviations from the current security posture, and that the details of who requested the change and why it was requested are documented.

NOTE: At the discretion of the Change Control Board, a request may require further analysis, for example, when a large number of assets are affected or there is a questions about compliance with regulatory standards.

Non-standard changes to baseline configurations are not permitted without approval by the Change Control Board unless an agency has requested and received an authorized Policy Exemption.

4.4 Analyze Security Impact of Configuration Changes

An agency must:

- Analyze the security impact of a proposed change and conduct security impact analysis prior to verifying a change to a configuration or an information system;
- Ensure the security impact level is scaled in accordance with the security categorization of the system (identify the risk high-water mark); and
- Review the security impact analysis to ensure that the approved, implemented changes did not have any unanticipated or adverse effects on the existing performance or security posture of the system.

4.5 Restrict Access for Implementing Changes

The system or information owner shall define, document, approve, and enforce physical and logical access to information and information systems subject to configuration changes.

- Only qualified and authorized individuals are allowed access to information systems for the purpose of making configurations changes and implementing upgrades.
- A list of qualified and authorized individuals shall be created and maintained to ensure the identification of individuals authorized to make changes to an information system.
- Access logs shall be created and maintained to ensure that configuration management is conducted as intended and to aid in post-configuration analysis.

4.6 Standardize Security-related Configuration Settings

Security-related configurations include, but are not limited to: rulesets, settings for ports and protocols, and directory settings such as access controls and group policy objects. When available, agencies shall use DISA STIGs as a best practice guide to establish baseline configurations.

Agencies shall:

- Establish and document configuration settings for information assets within their organizations that reflect the most restrictive mode consistent with operational requirements;
- Implement the configuration standardization;
- Monitor to ensure maintenance of mandatory configuration settings and track changes to configuration settings; and
- Document and maintain approved exceptions to the mandatory configuration settings, where applicable.

4.7 Configure Assets for Least Functionality

Information systems must be configured to provide only essential capabilities and to specifically prohibit or restrict the use of unauthorized ports, applications, or access. System owners must ensure:

- IT staff applies baseline configurations to all information systems
- Component functionality is limited to a single function per device, where possible, e.g., functionality may be for an email server or web server, but not both
  - For devices containing virtual components, see *Virtualization Policy*

4.8 Include Configuration Information in Asset Inventory

Inventory of information systems must be developed, documented, and maintained in accordance with the *Asset Management Policy*. This inventory of information technology assets will contain information on each asset's configuration, where possible. Inventory detail must be maintained at a level sufficient to enable tracking and reporting.

4.9 Manage Hardware and Software Lifecycles

Another aspect of configuration management is coordinating and establishing an asset life cycle process. Lifecycle management addresses the issues of maintaining an asset over its estimated “shelf life” in an organization. Factors specific to each organization’s business or mission are identified and prioritized to determine reasonable upgrade or replacement timelines as well as to budget plan over the long term. It allows the organization to identify yearly spending allotments for technology that account for device degradation, while ensuring production and efficiency are maintained. The primary security concern behind life cycle management focuses on data availability and protecting against data loss due to failing hardware.

The Enterprise Configuration Manager, coordinating with the Enterprise Requirements Manager, Enterprise Asset Manager, and DoIT Director of Infrastructure, will define a hardware and software life cycle process that accounts for the various IT assets utilized within the organization (for example workstations, mobile devices, servers, VoIP phones, printers, and even software such as operating systems that become obsolete or unsupported by the vendor). Agencies not actively managed by DoIT must also account for system development lifecycles. The requirements for this process are shown in the following table.

#	Name	Requirement
A	Asset Inventory	Perform a physical IT asset inventory (See *Asset Management Policy*).
B	Asset Prioritization	Determine IT asset priority, based on risk assessment and mission and business functions.
C	Identify Life Cycle Plan	Determine a lifecycle replacement plan for different categories of assets based on best practices. ▪ For example, current best practices indicate end user desktops be replaced every four to five years and servers every five to six years. (Best practice established by the International Association of Information Technology Asset Managers, Inc.).
D	Determine Current Shelf Life	Identify the current shelf life of deployed assets and verify against the asset priority to determine a course of action.
E	Asset Rollout Plan	Based on the lifecycle plan, the asset priority, and the current shelf life, begin financial planning for asset replacement.
F	Asset Deployment	Once assets have been purchased and integrated properly to the network, begin retirement of obsolete assets and deployment of new assets.

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an agency under the policy authority of DoIT requires an exemption from this policy then that agency must submit a DoIT Policy Exemption Request Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency’s mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Asset Management Policy
- Boundary Control and Internet Access Policy
- Patch Management Policy
- Virtualization Policy

7.0 Definitions

Term	Definition
Baseline Configuration	A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Change Control Board (CCB)	A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.
Configuration Management	Process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
Enterprise Configuration Manager	One who coordinates and maintains the process for establishing and ensuring consistency of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.
Enterprise Requirements Manager	One who manages the process of coordinating with stakeholders; analyzing, tracing, and prioritizing requests; and deciding on best course of action with relevant stakeholders.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for configuration management of Enterprise onboarded agencies. DoIT will manage configuration management according to established requirements as outlined in section 4.0 unless an agency has completed a Policy Exemption Request Form and received approval from DoIT. Agencies under the policy authority of the DoIT, but not under direct management, must manage configurations in such a way to meet the requirements established in section 4.0, unless a valid Policy Exemption Request Form has been approved by DoIT.

If DoIT determines that an agency is not compliant with this policy, the agency will be given a sixty (60) day notice to become compliant or at least provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated.

Any attempt to circumvent the configuration management policy, such as intentionally omitting, failing to record, or excluding configuration changes from inventory will be treated as a security violation and subject to disciplinary action which may include written notice, suspension, termination, and possible criminal and/or civil penalties.